

T E M P L A T E

Acceptable Use of AI Tools Policy

For [Company Name] · Version [1.0] · Effective [Date] · Owner: [Policy Owner, Title]

How to use this template: replace everything in **[green brackets]**, delete the industry sections in Appendix A that don't apply to you, and fill in the Approved Tools register in Section 5. Plan on about an hour.

This template describes IT and security best practices. It is not legal or regulatory advice. Have your attorney or compliance advisor review it before you adopt it, especially if you handle health, financial or government-contract information.

1. Why this policy exists

AI tools such as chat assistants, writing helpers, meeting note-takers and browser extensions can save our team real time. They also create a new way for confidential information to leave the company: anything typed, pasted or uploaded into an AI tool may be stored, reviewed or used by the tool's provider under its own terms.

This policy lets **[Company Name]** use AI productively while keeping client, patient, employee and company information under our control. It does not ban AI. It sets out which tools are approved, what information may go into them, and what to do when something goes wrong.

2. Who and what it covers

- Everyone who works for or on behalf of **[Company Name]**: employees, managers, owners, contractors, interns and temporary staff.
- Every AI tool used for company work, on any device: company computers, personal computers and phones, tablets, and devices in the shop or field.
- AI features built into software we already use (for example, AI features inside email, document, accounting, practice-management or design software), not only standalone AI apps.

3. Definitions

Term	Meaning in this policy
AI tool	Any software that generates text, images, audio, code, summaries or decisions from information you give it. Includes chat assistants, writing and grammar assistants, meeting recorders and note-takers, transcription apps, image generators, coding assistants and browser extensions with AI features.
Approved AI tool	A tool listed in the Approved Tools register (Section 5), used through a company-managed account with the settings listed there.
Personal or free AI account	Any AI account you created yourself, including free tiers of commercial tools. These are not approved for company information, even if the same product is approved under a company account.

Term	Meaning in this policy
Shadow AI	Any AI tool used for company work that is not on the Approved Tools register.
Confidential information	Any information in the Confidential or Restricted classes in Section 4.

4. What information may go into an AI tool

Before you type, paste, upload or record anything into an AI tool, decide which class it belongs to. When in doubt, treat it as the more sensitive class.

Class	Examples	Allowed in AI tools?
Public	Published marketing content, our public website, public regulations and standards, general how-to questions.	Yes, in any approved tool.
Internal	Internal procedures, meeting agendas, non-sensitive drafts, general business questions with names removed.	Yes, in approved tools only, through a company account.
Confidential	Client and customer files, contracts, pricing and bids, financial reports, employee information, unreleased plans, drawings and specifications, source code.	Only in tools the register marks "Confidential OK", and only for the purpose listed there.
Restricted	Patient or health information; Social Security, driver's license or passport numbers; bank, card or account numbers; passwords, keys and access codes; information covered by a government contract's handling rules; anything a client contract forbids sharing with third parties.	Never, unless the register names a specific tool approved for that data type in writing by [Policy Owner] , with the required agreements in place.

Removing names is not always enough. A description detailed enough that a colleague could identify the client, patient or employee is still Confidential or Restricted.

5. Approved Tools register

[Policy Owner] keeps this register current. If a tool is not listed, it is not approved.

Tool	Account type	Highest data class	Required settings	Approved for
[Tool name]	[Company / Enterprise]	[Internal / Confidential]	[e.g. training on our data turned off; company sign-in with MFA]	[e.g. drafting emails, summarizing internal documents]
[Tool name]	[]	[]	[]	[]
[Tool name]	[]	[]	[]	[]
[Tool name]	[]	[]	[]	[]

Before a tool is added to the register, [Policy Owner] confirms at least the following:

- Where the provider stores our information, and how long it keeps it.
- Whether the provider uses our information to train its models, and that this is turned off or excluded by contract.
- That accounts are managed by the company, use multi-factor authentication, and can be removed when someone leaves.
- That any agreement our obligations require is signed before Confidential or Restricted information is used (see Appendix A).

6. Rules for everyday use

Do

- Use only approved tools, signed in with your company account.
- Check the data class before you paste, upload or record anything.
- Read and check AI output before you use it. You are responsible for anything you send, file or act on, whoever or whatever drafted it.
- Say when AI drafted something if a client, patient or regulator would reasonably expect to know.
- Ask [Policy Owner] when you are unsure. Asking is always the right call.

Don't

- Don't use personal or free AI accounts for company work.
- Don't put Restricted information into any AI tool except as the register specifically allows.
- Don't install AI browser extensions, plug-ins or add-ons without approval. Many can read every page and email you open.
- Don't let AI make final decisions about hiring, firing, pay, credit, patient care, safety or legal matters. A qualified person decides.

- Don't rely on AI for facts, figures, citations, legal requirements or medical information without checking a reliable source.
- Don't paste content you don't have the right to share, such as another company's confidential documents.

7. Meeting recorders and note-takers

AI note-takers join calls, record audio and send transcripts to the provider. They need extra care:

- Only approved note-takers may be used, and only on meetings where they are listed as approved in the register.
- Everyone on the call must be told the meeting is being recorded and transcribed, and the host must get their agreement first. Florida generally requires the consent of all parties to record a conversation, and other states have their own rules.
- Never use a note-taker on calls where Restricted information will be discussed unless the register approves that tool for that information.
- Turn off auto-join features that let a note-taker join meetings you did not start.

8. Requesting a new tool

1. Send **[Policy Owner]** the tool's name, what you want to use it for, and the most sensitive class of information it would touch.
2. **[Policy Owner]** reviews the provider's terms and security settings against Section 5 and replies within **[5]** business days.
3. If approved, the tool is added to the register with its required settings, and an account is set up for you through the company.
4. Until it is approved, don't use the tool for company work, including in a free trial.

9. If information goes where it shouldn't

Mistakes happen. What matters is reporting them quickly so they can be contained. If you put Confidential or Restricted information into an unapproved tool, or into an approved tool beyond what the register allows:

1. Stop using the tool for that task. Don't try to fix it by deleting the chat on your own first; note what you entered and when.
2. Tell **[Policy Owner]** and **[IT contact]** within **[24 hours]** by **[phone / internal channel]**.
3. **[Policy Owner]** decides whether the event must be reported to clients, patients, insurers, regulators or contract officers, with legal advice where needed.

Reporting a mistake promptly will not, on its own, lead to disciplinary action. Hiding one may.

10. Training, review and enforcement

- Everyone covered by this policy reads it and signs the acknowledgment (Appendix B) when they start and whenever it changes.
- **[Policy Owner]** reviews this policy and the register at least every **[12]** months, and sooner when we adopt a major new tool or our obligations change.

- [Company Name] may monitor company systems and networks to detect unapproved AI tools, as allowed by law and our other policies.
- Breaking this policy may lead to disciplinary action, up to and including termination, under [Company Name]'s existing disciplinary process.

Appendix A: Industry add-ons

Keep the sections that apply to [Company Name]. Delete the rest.

A1. Healthcare practices, pharmacies and other HIPAA covered entities

- Patient information is Restricted. It may be used only in a tool whose provider has signed a Business Associate Agreement (BAA) with [Company Name] covering that use, and only for the purpose listed in the register.
- Free and personal AI accounts generally do not come with a BAA. Never use them with patient information.
- Record approved AI uses involving patient information in your HIPAA Security Risk Analysis and risk management plan.
- Veterinary practices: animal health records are not covered by HIPAA, but client names, contact details and payment information are still Confidential or Restricted.

A2. Legal, accounting, financial and engineering firms

- Client files are Confidential at minimum. Check engagement letters and client contracts for terms that forbid sharing with third-party services, and treat those clients' information as Restricted.
- Tax preparers and other firms covered by the FTC Safeguards Rule: list approved AI tools in your written information security program and include them in your risk assessment.
- Don't submit AI-drafted filings, opinions, calculations or stamped work without full review by the responsible professional.

A3. Property management and HOA/condo association management

- Owner and tenant financial information, applications, screening results and payment details are Restricted.
- Maintenance requests and tenant communications that identify a person or unit are Confidential.
- Check your property management software's built-in AI features against Section 5 before turning them on.

A4. Manufacturing, distribution and construction

- Drawings, specifications, bids, estimates, pricing, process recipes, machine programs and supplier terms are Confidential.
- Information received under a customer NDA follows that NDA. If the NDA forbids third-party processing, treat it as Restricted.
- Government contractors: information marked or defined as Federal Contract Information or Controlled Unclassified Information follows your contract's handling requirements and is Restricted. Don't put it into any AI tool unless your contract and your security plan specifically allow that tool.

Appendix B: Acknowledgment

I have read the [Company Name] Acceptable Use of AI Tools Policy, version [1.0]. I understand it, I agree to follow it, and I know whom to ask when I am unsure.

Name

Signature

Date